OUTLINE SHEET 6.1

Computer Security (Information Assurance (IA)) Program

REFERENCES

SECNAV M-5510.30, Chapter 2
SECNAV M-5510.36, Chapter 2, 6, and 12
SECNAV M-5239.1, DON Information Assurance Program
Interim DOD IA Certification and Accreditation Process (DIACAP),
  6 Jul 06
IA P-5239 Pub Series, Navy Staff Office (Naval Information
   Systems Management Center) Publications (Titles listed on
   INFOSEC Web page)
SECNAVINST 5720.47B, DON Policy for Content of Publicly
   Accessible World Wide Web Sites
OPNAVINST C5510.93F/MCO C5510.19, Navy/Marine Corps
   Implementation of National Policy on Control of Compromising
   Emanations (U)

OUTLINE

A.   Computer Security (Information Assurance (IA)) Program

  1.   Commander Naval Network Warfare Command (COMNETWARCOM)
        is the Navy's central operational authority for this
        program.

  2.   Scope: All DON activities, organizations and
        contractors using information systems or networks at
        DON activities and contractor operated or owned
        facilities under DON authority

  3.   Information Assurance (IA) (definition): The
        protection of information systems (IS) *against*:

        - Unauthorized access to or modification of
          information
        - Denial of service to authorized users, and
        - Providing service to unauthorized users

        NOTE: IA also includes measures necessary to detect,
        document, and counter those threats

  4.   Commands with information systems   **(ISP 2-7, PSP 2-8)**

    a.   CO designates, in writing, an Information Assurance Manager (IAM) who serves as POC for all command IA issues and implements command's IA program

    b.   CO also designates, in writing Information Assurance Officer(s) to implement and maintain command's network security requirements

5.   Program Objectives

    a.   Provide complete set of services to information systems developers and users

    b.   Provide systems security engineering and integration of critical IA products, techniques and designs into DON systems (NIPRNET and SIPRNET)

    c.   Protect the confidentiality, integrity, availability, authentication and non-repudiation (i.e., information assurance) of information (classified, privacy act, sensitive but unclassified and for official use only) and resources to the degree commensurate with their value

    d.   Employ efficient procedures and cost-effective, information-based security features to protect against *accidental* or *intentional* modification, disclosure, destruction, and/or denial of service; concerns are:

- Insider threat
- Hacker/Cracker
- Malicious code/viruses/worms
- State sponsored computer network attack
- Self-imposed or deliberate actions of others

(Viruses are a major concern. They can:
- Deliberately destroy documents/data files, put messages on screens or otherwise create a nuisance and interrupt work
- Be present in files, hidden on system areas of disks or even on disks that apparently contain no files

Adopt good, virus-aware habits

- Use special virus-detection software (can download from Navy INFOSEC Website https://infosec.navy.mil) along with anti-spyware and firewall protection
- Keep virus detection software updated by also downloading monthly signatures (updates) from the INFOSEC Web page
- Report all computer viruses to Navy Cyber Defense Operations Command (NCDOC) (previously known as NAVCIRT)
- Promptly eliminate viruses if found
- If get a virus do not operate computer until cleaned - if virus is on a workstation attached to a network disconnect until workstation checked

To protect against viruses

- Beware of an e-mail message with a binary file attachment - scan before opening
- Use a virus scanner that can eradicate macro viruses
- Install a memory-resident virus checker to detect suspicious program activity
- Regularly scan hard drive for viruses
- Scan anything you download off Net or online services
- Use several types of virus scanners
- Scan all portable media brought into your command
- Password protect systems
- Use only legitimate software obtained from a known source)

    e.   Conduct an assessment of threats, identify appropriate combination of safeguards and apply an appropriate level of certification and accreditation for each specific IS

B.   Certification and Accreditation

1.   Certification - A comprehensive evaluation of the technical and non-technical security features and other safeguards of a network or IS to establish extent to which a particular design and implementation meet a set of specified security requirements

2.   Accreditation - Formal declaration by a Designated Approving Authority (DAA) that a geographic site or an IS is approved to operate in a prescribed operational configuration using a defined set of safeguards and countermeasures against stated threats and vulnerabilities (NETWARCOM is the Navy DAA)

3.   DIACAP (DOD Information Assurance and Certification and Accreditation Process)- Promulgated by Interim DOD IA and Certification Guidance

    a.   Standardizes process used by <u>all</u> DOD activities and incorporates a formal, four-phased approach: Definition, Verification, Validation and Post Accreditation Phases

    b.   Benefits

        - "Designing-in" of appropriate level of security features into new and evolving systems (precludes later retrofit)
        - Reduces required security documentation through creation of a System Security Authorization Agreement (SSAA)
        - Enables reciprocity between various services/agencies
        - Establishes single process for all DOD

4.   Accreditation of systems - Essential to success of DON's IA Program

    a.   Additional aspects

- Personnel security - Access based on individual's loyalty, reliability and trustworthiness
- Physical security - Protection from damage, loss, theft, or unauthorized physical access
- Procedural security - Ensure continuous operation of system/network
- Education, training and awareness

    b.   If a system is not yet accredited, but must become operational, an Interim Approval to Operate (IATO) must be issued by the DAA

C.   Processing of Controlled Unclassified Information and Classified Information on Information Systems

    1.   All DON information systems are designated as sensitive regardless of whether information processed is classified or unclassified

        a.   Information entered, stored or transmitted will not exceed the approved classification or sensitivity level for the system or network

        b.   All systems must have some type of access control system (normally passwords are used) to ensure only authorized personnel have access

    2.   Controlled unclassified information

        a.   Information which, although not classified, its loss, misuse, unauthorized access to, or modification of could adversely affect: the national interest; conduct of Federal Programs; or privacy of DOD personnel

        b.   Examples: Privacy Act Information, Financial Information, Medical Records, Proprietary Information, For Official Use Only (FOUO)

    3.   Classified Information – Can only be processed and stored on a system/network which meets the requirements for classified processing

        a.   Stand-alone systems must either have removable hard drives which can be removed and stored in an authorized security container, or be located in a

vault/secure room authorized for open storage at
the level being processed

b.   Network systems shall:

- Meet the encryption and cabling requirements
- Have the server located in a vault/secure room
  authorized for open storage at the level of the
  server
- Individual workstations shall either have
  removable hard drives or be located in a
  vault/secure room authorized for open storage
  at the level of the network

c.   Meet the requirements of NAVSO (IA) PUB 5239-22,
     Protected Distribution System (PDS). If system
     is located in a:

- <u>Secure room</u> - A PDS is not required for
  classified information processed at or below
  the authorized "open storage" level for a
  secure room or vault
- <u>Controlled Access Area (CAA)</u> – A PDS will not
  be required for classified information
  processed at or below the level of the
  classification level of the CAA. Unprotected
  cables may be run within, but not outside the
  perimeter of the CAA
- <u>Restricted Access Area (RAA)</u> – A PDS and lock
  box equipped with an approved PDS lock is
  required.

d.   Emanations Security (TEMPEST) Requirements

(1) Governing instruction: OPNAVINST
     C5510.93F/MCO C5510.19

(2) TEMPEST Policy - National security
     information will not be compromised by
     exposure to unauthorized interception of
     compromising emanations from Classified
     Information Processing systems

(3) Procedures for TEMPEST certification are
     outlined in the TEMPEST instructions

(4)   SPAWAR Systems Center, Charleston SC manages DON's TEMPEST program. Contact the help desk (Integrated Support Center) for assistance: 1-800-304-4636/COMM (843) 218-5550/DSN 588-5550/TOLL FREE 1-877-477-2927; email iscchas@spawar.navy.mil

D.   Marking Equipment, Media and Hard Copy   (ISP 6-34, 6-3353, Exhibit 6A-20 & 21)

1.   Removable computer storage media and devices (i.e., external hard drives, zip drives, CD-ROM's, disk cartridges, cassettes, diskettes magnetic disk packs/drives), thumb drives containing classified information:

   a.   Mark using color coded labels: SF 706 (TS); 707 (S); 708 (C); 710 (U); 712 (SCI)

   b.   Mark with labels on front only to clearly indicate highest overall classification level of the information they contain

   NOTE: When approved labels are not feasible due to interference with operation of the system or because of size of media, other means for marking may be used as long as they appropriately convey the classification and other required markings

2.   Equipment/Hardware (non removable)

   a.   Marking externally with highest overall level of information it stores/possesses is optional

   b.   If used, marking may be electronically stamped, printed, etched, written, engraved, painted, SF label, tag sticker, decal, or other similar device

3.   Internal Markings

   a.   Program systems processing classified information to clearly show appropriate classification level and associated markings when information is reproduced/generated, to include email sent over a classified system

    b.   IAMs and IAOs will ensure that all systems provide for classification designation of data stored in internal memory or maintained on fixed storage media

4.   Hard copy - Mark per the requirements for marking any other documents if it contains controlled unclassified or classified information

E.   Use of Portable Electronic Devices (CNO 272200Z APR 01)

1.   Portable Electronic Device (PED) – Generic title used to describe the myriad of small electronic items widely available for purchase

    a.   Becoming difficult to differentiate between these devices as trend is to combine capabilities and functions in various forms/formats

    b.   Ability of PEDs to directly interface with other devices and networks via radio frequency, infrared, and cable connections becoming more common

2.   Policy guidance applies to all PEDs to include pagers, mobile/cell phones, personal digital assistants/job performance aids, laptop/notebook computers, digital imagery (still/video) devices and devices of similar capability, functionality or design

3.   Non-Navy owned PEDS <u>are prohibited</u> from handling U.S. government protected information (classified information, restricted and sensitive but unclassified data/information)

4.   Navy-owned PED use is authorized, as detailed below, provided a conscious decision is made by cognizant security authority concerning managing risks associated with their use and use is governed by appropriate policy.

    a.   May be used to handle U.S. government protected information (classified information, restricted and sensitive but unclassified data/information) provided the PED meets security requirements for that mode of operation, data sensitivity, and classification level of material

    b.   Will <u>not</u> be connected to systems processing U.S.
          government protected information without
          permission of designated AIS accreditation
          authority/senior security authority

    c.   Will be safeguarded at same level of the
          protected information system

5.   All PEDs containing wireless communications or
      connectivity capability, audio, video, photographic
      recording and/or transmission capabilities will be
      restricted from areas where U.S. government protected
      information is processed or discussed, except when
      approved by senior cognizant security authority, based
      on a risk assessment and appropriate security
      countermeasures

F.   Electronic Spillage of Classified Information   (ISP 12-1)

1.   Definition – When data is placed on an IT system
      possessing insufficient information security controls
      to protect the data at the required classification
      (e.g., Top Secret spillage onto Secret, Secret onto
      UNCLAS, etc.)

2.   Upon discovery of an electronic spillage, due
      consideration must be given to the possibility of loss
      or compromise of classified information

3.   Prompt and complete identification and reporting
      facilitates rapid containment of the spillage and
      helps determine:

      - How the spillage occurred
      - Possible impact on Navy operations
      - Insight into how to prevent future occurrences

4.   If a spillage occurs:

    a.   All commands affected by the spillage (to include
          the originating command) will follow reporting
          procedures per current NETWARCOM guidance

b.   If the spillage results in the compromise of classified information, the Security Manager will ensure the procedures outlined in Chapter 12, ISP are properly followed for reporting compromise of classified information

G.   Role of NCDOC (previously NAVCIRT) and NCIS in IA

1.   CNO Washington DC 111754Z Oct 95 (ALCOM 045/95) established policy for computer incident response and vulnerability reporting (current guidance is OPNAVINST 2201.2)

a.   Security Incident - An attempt to exploit DON information systems or networks which can result in compromise of information, denial of service and other related disruptions which can severely impact on fleet operations.

b.   Incidents include: Penetration of computer Systems; introduction of technical and administrative vulnerabilities; introduction of computer viruses and other forms of malicious code

2.   Responsibilities of NCDOC

a.   Provide effective and timely technical response to security incidents

b.   Establish and operate an incident response team capability to centrally coordinate actions involving security incidents and vulnerabilities that threaten DON systems

c.   Review all reported DON information system and networking vulnerabilities and incidents and evaluate requirement for follow-up actions

d.   Facilitate reporting of security incidents involving violations of law to NCIS

e.   Coordinate with COMNAVSECGRU and ONI on incidents on SCI systems

3.   NCIS – Cyber Unit

       a.   Coordinate closely with NCDOC and operate the DON
            Computer Crime Hotline, 1-800-278-9917

       b.   Investigate intrusions, targeting or
            vulnerability incidents (including the foreign
            threat), computer theft and misuse of DON
            computer systems for criminal prosecution

H.   Worldwide Web Policy (SECNAVINST 5720.47B)

   1.   Determines that:

       a.   Some information on publicly available DON Web
            sites provided too much detail on naval
            capabilities, infrastructure, personnel and
            operational procedures

       b.   Such detail, when combined with other sources,
            may increase the vulnerability of DOD systems and
            potentially be used to threaten or harass naval
            personnel and their families

   2.   All COs who establish publicly accessible Web sites
       must ensure:

       a.   Information published on command's Web site does
            not compromise national security or place DOD
            personnel at risk

       b.   Command's Web site does not contain any of the
            information prohibited by SECNAVINST 5720.47A

       c.   Web site is formally accredited

I.   Information Warfare and Cyberterrorism

   1.   Two relatively new terms - Result of the vastly
       expanding use of computers

   2.   Information Warfare - Any action which attacks,
       protects, or uses military information functions or
       operations

       a.   Encompasses everything from electronic jamming to
            psychological operations

        b.   Can be remotely conducted from anywhere in the
world, with minimal risk to the individual,
organization or country because it is difficult
to pinpoint for attack/retaliation

   3.   Cyberterrorism - Environment where at the stroke of a
key millions of lives can be changed or destroyed
simply to prove a religious, political or ideological
point

        a.   Term which is not yet fully defined or the full
ramifications known

        b.   Applying automation to the concept of terrorism
by assassination, bombing, kidnappings, hijacking
and other means

        c.   Terrorists could utilize aspects of information
warfare to achieve their goal, such as:

           - Changing/altering records/files
           - Disrupting services
           - Disrupting information systems with viruses,
             trap doors, Trojan horses, malicious logic

        d.   Potentially as an attack method - it could prove
relatively cheap, safe and profitable for
terrorists

J.   Additional IA Program Safeguards

- Protect your password
- Mark and store IS media per its classification level
- Enforce copyright laws
- Place monitor so it cannot be viewed by unauthorized
  personnel
- Do not connect information systems that process
  classified information to unsecured modems
- Ensure computer is "wiped" and signed off by IAM before
  turning it into DRMO
- **<u>Never</u>** process classified information using personally
  owned hardware and software